Manual de usuario

Activación de certificado SSL

SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL, S.A.

Powered by

La Concepción - Río Palora OE2-37 Av. Amazonas – Telf.: (593-2) 2438 911 Fax: (593-2) 2250 271
www.securitydata.net.ec – 1800 FIRMAS
Quito-Ecuador

Una vez que haya obtenido los dos códigos (Número de Referencia y Código de Autorización) para la emisión del Certificado SSL, usted debe generar la solicitud de su servidor:

Windows Server IIS 7.5:

1. Abrir la consola de administración del IIS.
2. Dentro de las características del Servidor, seleccionar la opción **Server Certificates**.
3. En el panel **Actions**, seleccionar la opción **Create Certificate Request**
4. En la ventana que se despliega **Request Certificate** colocar la información que se indica a continuación:
    a. Common Name: NÚMERO DE REFERENCIA (Proporcionado por Security Data)
    b. Organization: Nombre de la Empresa
    c. Organizational Unit: Área a aplicar el Certificado
    d. City/Locality: Su ciudad
    e. State/Province: Su provincia
    f. Country/región: Su país
5. A continuación dar click en **Siguiente**.
6. Guardar el archivo en el Disco.
7. Ir a ka página de emisión: https://emision.securitydata.net.ec
8. Seleccionar en la menú Izquierdo la opción **SSL** o en el principal la opción **Crear Certificados SSL para Servidores Web desde una solicitud PKCS#10**
9. Ingresar los dos códigos proporcionados
    a. Número de Referencia
    b. Código de Autorización
10. En **opciones** seleccionar Visualizar en código PEM del formato raw DER.
11. En el cuadro inferior colocar la solicitud creada anteriormente copiando ---BEGIN CERTIFICATE REQUEST--- hasta ---END CERTIFICATE REQUEST---, verificar que no exista espacios al final.
12. Seleccionar la opción **Emitir Certificado**
13. En la siguiente ventana aparece el certificado codificado, para lo cual debe abrir el NOTEPAD y copiar desde ---BEGIN CERTIFICATE--- hasta ---END CERTIFICATE---, sin dejar espacios y guardar con un **nombre.cer**, adicional colocar en Guardar como ALL FILES o TODOS LOS ARCHIVOS, también puede Descargar el certificado dirigiéndose a la parte inferior de la página.
14. Una vez realizado el procedimiento se emite el certificado, el mismo que se instalará en el servidor en su aplicación.
15. Adicional instalar los certificados raíces, los cuales pueden ser descargados de la página web www.securitydata.net.ec en la sección Descargas.

Linux Server:

1. Instalar **openssl** y el **módulo ssl** de cada aplicación.
2. En consola de comandos.
3. Generar la llave privada del Servidor y la solicitud se debe ejecutar el comando siguiente: **openssl req -nodes -newkey rsa:2048 -keyout new-digitss.key -out new-digitss.csr**
4. El servidor solicita ingresar la siguiente información:
    a. Country Name: EC
    b. State of province Name: Su provincia
    c. Locality Name: Su ciudad
    d. Organization Name: Nombre de la Empresa
    e. Organizational Unit Name: Área a aplicar el certificado
    f. Common Name: NÚMERO DE REFERENCIA (Proporcionado por Security Data solo son números no hay letras ni signos)
    g. Email Address: Dirección de correo electrónico del Administrador
    h. Y en los otros campos ENTER sin información.
5. Se generan dos archivos **server.key** y **server.csr.**
6. Se encuentra lista la solicitud de certificado y la llave privada
7. Ir a la página de emisión: https://emision.securitydata.net.ec
8. Seleccionar en la menú Izquierdo la opción **SSL** o en el principal la opción **Crear Certificados SSL para Servidores Web desde una solicitud PKCS#10**
9. Ingresar los dos códigos proporcionados
    a. Número de Referencia
    b. Código de Autorización
10. En **opciones** seleccionar Visualizar en código PEM del formato raw DER.
11. En el cuadro inferior colocar la solicitud creada anteriormente que se encuentra dentro del archivo **server.csr** copiando ---BEGIN CERTIFICATE REQUEST--- hasta ---END CERTIFICATE REQUEST---, verificar que no exista espacios al final.
12. Seleccionar la opción **Emitir Certificado.**
13. En la siguiente ventana aparece el certificado codificado, para lo cual debe abrir el NOTEPAD y copiar desde ---BEGIN CERTIFICATE--- hasta ---END CERTIFICATE---, sin dejar espacios y guardar con un **nombre.crt**, adicional colocar en Guardar como ALL FILES o TODOS LOS ARCHIVOS.
14. Una vez realizado el procedimiento se emite el certificado, el mismo que se instalará en el servidor en su aplicación.
15. Adicional instalar los certificados raíces en formato PEM con extensión **.CRT o .PEM,**
16. Si es en formato .CRT instalar los certificados raíces, los cuales pueden ser descargados de la página web www.securitydata.net.ec en la sección Descargas.